# The forth national conference on combinatorial designs and their applications

## Program

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Session</th>
<th>Chair</th>
<th>Talks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012.6.16</td>
<td>8:10-8:15</td>
<td>Opening Ceremony</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8:15-9:15</td>
<td>Talks</td>
<td>Chair: Jianxing Yin</td>
<td>Charles Colbourn: Resolvable covering arrays and their applications</td>
</tr>
<tr>
<td></td>
<td>9:15-9:45</td>
<td>Tea Break and Photos</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>9:45-10:45</td>
<td>Talks</td>
<td>Marco Buratti</td>
<td>A collection of cyclotomic conditions for the existence of some combinatorial designs</td>
</tr>
<tr>
<td></td>
<td>10:45-10:55</td>
<td>Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10:55-11:55</td>
<td>Talks</td>
<td>Violet Syrotiuk</td>
<td>Using Locating Arrays for Screening Experiments</td>
</tr>
<tr>
<td></td>
<td>11:55-1:30</td>
<td>Lunch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012.6.17</td>
<td>2:00-2:30</td>
<td>Talks</td>
<td>Chair: Jianguo Lei</td>
<td>Minquan Chen: Optimal Separable Codes</td>
</tr>
<tr>
<td></td>
<td>2:30-3:00</td>
<td>Talks</td>
<td>Dameng Deng</td>
<td>Derandomization by Conditional Probabilities and its Applications to Some Combinatorial Covering Problems</td>
</tr>
<tr>
<td></td>
<td>3:00-3:30</td>
<td>Talks</td>
<td>Cuiling Fan</td>
<td>Comma-free codes and difference systems of sets</td>
</tr>
<tr>
<td></td>
<td>3:30-3:45</td>
<td>Tea Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3:45-4:15</td>
<td>Talks</td>
<td>Tao Feng</td>
<td>Semi-cyclic Steiner quadruple systems</td>
</tr>
<tr>
<td></td>
<td>4:15-4:45</td>
<td>Talks</td>
<td>Ce Shi</td>
<td>Combinatorial Properties and Constructions of Locating and Detecting Arrays</td>
</tr>
<tr>
<td></td>
<td>4:45-5:15</td>
<td>Talks</td>
<td>Xiaomiao Wang</td>
<td>Optimal OOCs with unequal auto- and cross-correlation constraints</td>
</tr>
<tr>
<td></td>
<td>5:45-7:30</td>
<td>Dinner</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012.6.17</td>
<td>8:30-9:30</td>
<td>Talks</td>
<td>Chair: Keqing Feng</td>
<td>Cunsheng Ding: Cyclic Codes from Difference Sets and Almost Difference Sets</td>
</tr>
<tr>
<td></td>
<td>9:30-9:45</td>
<td>Tea Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>9:45-10:45</td>
<td>Talks</td>
<td>Fangwei Fu</td>
<td>Subspace Codes for Network Error Correction</td>
</tr>
<tr>
<td></td>
<td>10:45-10:55</td>
<td>Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10:55-11:25</td>
<td>Talks</td>
<td>Pinghui Ke</td>
<td>On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$</td>
</tr>
<tr>
<td></td>
<td>11:25-11:55</td>
<td>Talks</td>
<td>Changli Ma</td>
<td>The minimum distances of some classes of LDPC codes</td>
</tr>
<tr>
<td></td>
<td>11:55</td>
<td>Lunch</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
One-hour Talks

A collection of cyclotomic conditions for the existence of some combinatorial designs

Marco Buratti
Università di Perugia

Abstract: In this talk I will give an overview on cyclotomic conditions guaranteeing the existence of some combinatorial designs with a nice automorphism group. I will show, in particular, a quite close connection of this subject with the factorization theory of groups.

Resolvable Covering Arrays

Charles J. Colbourn
Arizona State University

Abstract: Two powerful recursive constructions of covering arrays of strengths three and four use difference covering arrays (DCAs). However, what is required in these constructions is not the algebraic structure of differences in a group, but rather that the DCAs produce covering arrays that are resolvable. Both constructions are strengthened by using resolvable covering arrays in place of DCAs.

First, we develop computational methods for finding resolvable covering arrays, primarily by extending techniques for difference covering arrays. We also develop some recursive techniques for producing resolvable covering arrays. Secondly, we explain the use of these resolvable arrays in applying recursive techniques for covering arrays. Improvements for bounds on covering array numbers are shown to be substantial.

A number of open problems are introduced.

Cyclic Codes from Difference Sets and Almost Difference Sets

Cunsheng Ding
Department of Computer Science and Engineering
Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong, China

Abstract: Cyclic codes are a subclass of linear codes. The error correcting capability of cyclic codes may not be as good as linear codes in general. However, many cyclic codes are optimal linear codes in the sense that they meet certain bounds on parameters of linear codes. Cyclic codes have wide applications in storage and communication systems because
they have efficient encoding and decoding algorithms. For example, Reed-Solomon codes have found important applications from deep-space communication to consumer electronics. They are prominently used in consumer electronics such as CDs, DVDs, Blu-ray Discs, 2D-bar codes, in data transmission technologies such as DSL & WiMAX, in broadcast systems such as DVB and ATSC, and in computer applications such as RAID 6 systems.

Almost difference sets and difference sets are interesting topics of combinatorial designs and have applications in many areas of mathematics and engineering fields.

In this talk, we will introduce cyclic codes derived from almost difference sets and difference sets, summarize known results, and present a number of open problems.

Subspace Codes for Network Error Correction

Fangwei Fu
Nankai University

Abstract: Subspace codes was introduced by Koetter and Kschischang in 2007 as network error-correcting codes. Constant dimension codes is an important class of subspace codes. In this talk, we review and survey some bounds and constructions for constant dimension codes. In particular, it is shown that constant dimension codes achieve the Wang-Xing-Safavi-Naini bound if and only if they are certain Steiner structures. We point out that a family of known Steiner structures is actually a family of optimal constant dimension codes. Finally, we present some open problems.

Using Locating Arrays for Screening Experiments

Violet Syrotiuk
Arizona State University

Abstract: In complex and dynamic systems, the exhaustive test suite (the full-factorial design) is too large and hence methods are sought to reduce the number of experiments required to identify important factors and interactions. Reduction relies on a sparsity of effects assumption; that interactions of interest involve at most a small, known number $t$ of interacting factors. As one means of reduction, locating arrays have recently been defined. For a set of factors each taking on a known number of levels, a locating array permits the identification of a small number of significant interactions among small sets of (factor, level) combinations; each experiment in the test suite consists of a choice of level for each factor. They differ from standard designed experiments, which are used to measure interactions and to model the performance as a function of these. In this talk, we present the use of locating arrays for factor screening experiments in mobile ad hoc networks.
Optimal Separable Codes

Minquan Cheng
School of Mathematical Sciences
Guangxi Normal University

Abstract: Cheng and Miao (2011) introduced separable code, which can be used in multimedia fingerprinting resistant to linear collusion attacks on multimedia contents. In this talk, we first derive several upper bounds on the sizes of \( t \)-separable codes, and then turn our attention to the constructions of optimal \( \mathcal{F} \)-separable codes with short length. Two infinite families of optimal \( \mathcal{F} \)-separable codes of length 2 are constructed from projective planes, and all optimal \( \mathcal{F} \)-separable codes of length 3 are explicitly constructed by means of difference matrices.

Derandomization by Conditional Probabilities and its Applications to Some Combinatorial Covering Problems

Dameng Deng
Shanghai Jiaotong University

Abstract: The probabilistic method is a powerful tool for tackling many problems in discrete mathematics. It can be used to get existence results for lots of combinatorial problems. But in general, the method is non-constructive. In this paper, we use the method of conditional probabilities as a unified derandomization method for a set of combinatorial covering problems, including splitting systems, perfect hash families, cover-free families, and \( \Delta \)-free systems, thus getting efficient algorithms to construct these combinatorial structures deterministically.

Comma-free codes and difference systems of sets

Cuiling Fan
Nantong University

Abstract: Difference systems of sets were introduced by Levenshtein and were used for the construction of comma-free codes that allow for syncrhonization in the presence of errors. This talk mainly summarizes most of the known constructions of difference systems of sets and the relationship between difference systems of sets and other combinatorial designs.
Semi-cyclic Steiner quadruple systems

Tao Feng
Institute of Mathematics, Beijing Jiaotong University
Beijing 100044, P. R. China
E-mail: tfeng@bjtu.edu.cn

Abstract: Let \( K \) be a set of positive integers and \( t \) a positive integer. A \( t \)-wise balanced design (tBD) is a pair \((X, B)\), where \( X \) is a set of \( v \) points and \( B \) is a set of subsets of \( X \) (called blocks), each of cardinality from \( K \), such that every \( t \)-subset of \( X \) is contained in exactly one block. Such a design is denoted by \( S(t, K, v) \). When \( K = \{ k \} \), we simply write \( k \) for \( K \). An \( S(3, 4, v) \) is called a Steiner quadruple system and denoted by SQS\((v)\).

An automorphism \( \alpha \) of a \( t \)-wise balanced design \((X, B)\) is a permutation on \( X \) leaving \( B \) invariant, i.e., \( \{ \alpha(x) : x \in B \} = B \). An \( S(t, K, u \times v) \) is said to be semi-cyclic or \( v \)-cyclic (denoted by \( S(t, K, u \times v) \)) if it admits an automorphism \( \pi \) consisting of \( u \) cycles of length \( v \). Without loss of generality identify \( X \) with \( I_u \times Z_v \) and the automorphism \( \pi \) can be taken as \((i, x) \mapsto (i, x + 1) \mod (v, v)\), \( i \in I_u \) and \( x \in Z_v \).

All automorphisms of an \( S(t, K, v) \) form a group, called the full automorphism group of this \( S(t, K, v) \). Any subgroup of the full automorphism group is called an automorphism group of this \( S(t, K, v) \). Let \( G \) be an automorphism group of an \( S(t, K, v) \). For any block \( B \) of the \( S(t, K, v) \), the subgroup \( \{ \pi \in G : B^{\pi} = B \} \) is called the stabilizer of \( B \) in \( G \). If the stabilizer of each block of a semi-cyclic \( S(t, K, u \times v) \) is trivial in \( Z_v \), i.e., for each block \( B \), \( \delta \in Z_v : B + \delta = B \) is trivial, \( \{ (i, x + \delta) : (i, x) \in B \} \), then this \( S(t, K, u \times v) \) is called strictly semi-cyclic. When \( u = 1 \), a (strictly) semi-cyclic \( S(t, K, 1 \times v) \) is often simply referred to as a (strictly) cyclic \( S(t, K, v) \). When \( v = 1 \), a (strictly) semi-cyclic \( S(t, K, u \times 1) \) is just a \( S(t, K, u) \). We shall show that in order to solve the existence problem of strictly semi-cyclic \( S(3, 4, u \times v)s \), one can only example the existence of strictly semi-cyclic \( S(3, 4, 1 \times v)s \) (i.e., strictly cyclic \( SQS(v) \)) and strictly semi-cyclic \( S(3, 4, 2 \times v)s \).

Furthermore, some direct and recursive constructions for strictly cyclic \( SQS(v)s \) and strictly semi-cyclic \( S(3, 4, 2 \times v)s \) are mentioned.

On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length \( 2^p m \)

Pinghui Ke
Fujian Normal University

Abstract: Due to their nice algebraic structure, cyclotomic methods had been widely used in combinational design, coding and cryptography et al. In this report, new classes of generalized cyclotomic binary sequences with period \( 2^p m \) are proposed. We determine the linear complexity and autocorrelation of these sequences.
The minimum distances of some classes of LDPC codes

Changli Ma
The College of Mathematics and Information Science
Hebei Normal University

Abstract: Some classes of LDPC codes are constructed based on finite geometry. P. Sin and Q. Xiang determined the dimensions of these codes in some cases. Recently, we determined their minimum distances.
Joint work with Feng Ya’nan, Wang Lu and Deng Shuo.

Combinatorial Properties and Constructions of Locating and Detecting Arrays

Ce Shi
Suzhou University

Abstract: Locating and detecting arrays were introduced by Colbourn and McClary in 2008, which are of interest in generating software test suites to locate and detect interaction faults in component-based systems. In this talk, combinatorial properties and constructions of locating and detecting arrays are presented. As a consequence, a great number of locating and detecting arrays are constructed, which are all optimal in the sense of their sizes.

Optimal OOCs with unequal auto- and cross-correlation constraints

Xiaomiao Wang
Ningbo University

Abstract: Optical orthogonal codes (OOCs) are commonly used as signature codes for optical code-division multiple access systems. So far, research on optical orthogonal codes has mainly concentrated on the same auto-correlation and cross-correlation constraints. In this talk, we are concerned about optimal optical orthogonal codes with the auto-correlation $\lambda_a$ and the cross-correlation 1. Some optimal one-dimensional OOCs and two-dimensional OOCs are obtained.